REMARKS/ARGUMENTS

Claims 1-5, 7-11, 13-16, 18-22, 24, 25, 29, 30, and 32 are pending.

Claims 1-5, 7-11, 13-16, 18-22, 24, 25, 29, 30, and 32 were rejected under 35 U.S.C. 102(e) for allegedly being anticipated by Downs et al.

The present invention relates to authentication over a communication network. Aspects of the present invention include providing "enhanced content" produced at a first processing apparatus and communicating it to a user at a second processing apparatus. *Claim 1.* The enhanced content is produced by "combining content and said identifier." *Claim 1.* The enhanced content is then presented to the user. As recited in other claims, "presentation" is an action where the enhanced content "is displayed to a user." *Claim 5, see also for example claim 8 "means for displaying", claim 11 "upon displaying said enhanced contents to a user", and claim 14 "display means".* The identifier is visually imperceptible when the enhanced content is displayed to the user.

The identifier can then be extracted from the enhanced content and used to generate input data that is transmitted from the second processing apparatus. For example, claim 1 recites "said input data is produced based on said identifier; and transmitting said input data from said second information apparatus to said first information apparatus." Kindly refer also to independent claims 14, 19, 22, 24, 29, and 32.

In another aspect of the present invention, the identifier can be used to determine whether to invalidate a previously stored identifier. For example, claim 5 recites "invalidating said stored identifier if said acquired identifier matches said stored identifier" where the "acquired identifier" is the extracted identifier. Kindly refer also to independent claims 8, 11, 16, and 21.

A review of the reference to Downs et al. does not reveal the present invention as recited in the pending claims. As cited by the Examiner, Downs et al. summarize in column 3, lines 42 - 55 a technique for securely providing encrypted data to a user. A decryption key ("KEY") that is used to decrypt the encrypted data is encrypted using a first public key. The encrypted KEY is sent to a clearing house, which then performs a decryption operation using a

private key that corresponds to the first public to obtain the KEY. The KEY is then re-encrypted using a second public key. The re-encrypted KEY is sent to the user. The user possesses a private key that corresponds to the second public key. The second private key is applied by the user to perform a decryption operation to obtain the KEY. The user can then decrypt the encrypted data using the obtained KEY.

It is not clear in the Office action which aspects of the present invention are purportedly taught by this cited portion of Downs et al. However, from the foregoing summary by Downs et al., it can be seen that there is no discussion of receiving "enhanced data" that is "presented" or "displayed" to the user such that the identifier is visually imperceptible. The clearing house in Downs et al. transmits an encrypted KEY to the user; there is no indication that the encrypted key is "displayed" to the user. There is no discussion of the user extracting an identifier from the encrypted data. Downs et al. only mention that the decrypts the encrypted KEY and uses it to decrypt the encrypted data.

Downs et al. were cited at column 10, lines 50 - 67. Here, Downs et al. describe in further detail the processing that occurs in the clearing house. The clearing house provides authentication and record keeping functions. The clearing house also receives a request from a user for a decryption key. In response, the clearing house sends the decryption key to the user encrypted in a manner that only the user can decrypt it.

While it is not clear in the Office action which aspects of the present invention are purportedly taught by this cited portion of Downs et al., it appears that the clearing house was cited for teaching "enhanced content." However, the clearing house sends an encrypted key to the user. It is respectfully submitted that an encrypted key is not the same as "enhanced content" that comprises a combination of "content and said identifier." *Claim 1.* In addition, there is no suggestion that the encrypted decryption key is "displayed" to the user, whereas the "enhanced content" is displayed to the user in the present invention.

Downs et al. were cited at column 14, lines 19 - 28 where they discuss the general idea of a "digital certificate," a conventional authentication technique used to authenticate or verify the identity of a person or entity that has sent a digitally signed message. A certificate is a

digital document issued by a certification authority that binds a public key to a person or entity. The certificate includes the public key, the name of the person or entity, an expiration date, the name of the certification authority, and other information. The certificate also contains the digital signature of the certification authority. When an entity (or person) sends a message signed with its private key and accompanied with its digital certificate, the recipient of the message uses the entity's name from the certificate to decide whether or not to accept the message.

It is not clear in the Office action which aspects of the present invention are purportedly taught by this cited portion of Downs et al. At best, it seems the digital certificate relates to the "enhanced content" recited in the pending claims. However, the idea of a digital certificate in and of itself does not suggest much beyond that to obtain the present invention. The idea of a digital certificate does not suggest that the encrypted message be displayed. The idea of a digital certificate does not suggest that the certificate itself be used to generate "input data" that is sent back to the sending computer (claim 1), or to invalidate a previously stored identifier (claim 5).

Downs et al. were cited at column 25, lines 57 - 60 and column 25, line 65 to column 26, line 3. With respect, it is not clear how these cited portions teach or suggest any aspect of the present invention as recited in the independent claims. The description relates to data fields in a secure container (SC). Column 25, lines 57 - 60, for example, describes a field that is used to identify an encryption key or an encrypted form of a decryption key. Column 25, lines 65 and following describe a field that identifies an encryption that is used to encrypt the decryption key. It is earnestly submitted that this portion of the Downs et al. reference neither teaches or suggests the present invention as recited in the pending claims.

Downs et al. were cited in column 29, lines 29 - 61 where fields in a metadata SC table are described. *Col. 29, lines 16 - 17.* They describe a Content ID field which defines a unique ID that is associated with a content item. They describe Metadata field which is information related to a content item such as artist name. They describe a Usage Condition field which describes usage restrictions imposed on the user. They describe an SC Templates field

which describes information relating to ordering and licensing the content. They describe a Watermarking Instructions field which pertain to watermarking the content.

With respect, it is not clear how these data fields teach or suggest any aspect of the present invention as recited in the independent claims. At most, the watermarking discussion bears some relation to the present invention. However, the watermarking discussion does not teach or suggest that the recipient of the "enhanced content" extract an identifier from the enhanced content and use it to produce "input data" that is then sent back to the sending computer (claim 1). The watermarking discussion does not teach or suggest that the recipient of the "enhanced content" extract an identifier from the enhanced content and use it to invalidate a previously stored identifier (claim 5).

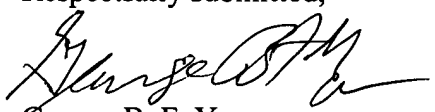
It is earnestly submitted that Downs et al. do not teach or suggest the present invention as recited in the pending claims. The Section 102 rejection of the claims is believed to be overcome. Reconsideration of the claims in view of the foregoing remarks is respectfully requested.

CONCLUSION

In view of the foregoing, all claims now pending in this Application are believed to be in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



George B. F. Yee
Reg. No. 37,478

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
GBFY:cmm
60287121 v1